Basic IT Security

You are the number one reason your agency is safe

“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”
— Stephane Nappo

Global Chief Information Security Officer Société Générale International Banking

“In the underworld, reality itself has elastic properties and is capable of being stretched into different definitions of the truth.”
— Roderick Vincent, The Cause

Focus: Password Security

The strongest door is meaningless if someone has the key to it.

The focus of this session is specifically on Password Security, as the fundamental first step in protecting your agency.

Do Not Share Your Password

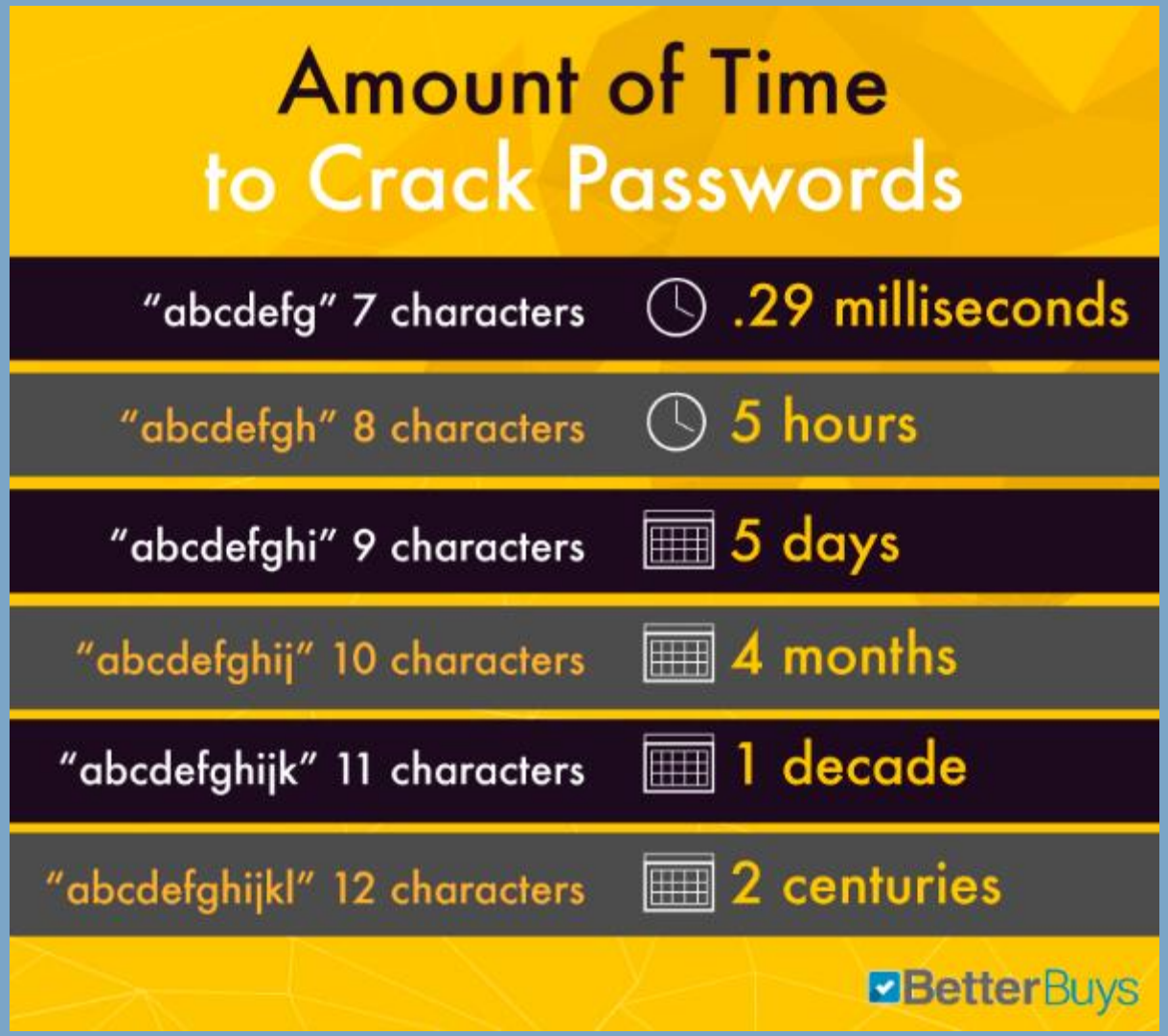
According to the Center for Internet Security

Passwords are a major defense against hackers, and developing good password practices will help keep your sensitive personal information and identity more secure.

Tips for Developing Better Passwords:

- Passwords should have at *least* 10 characters, include uppercase and lowercase letters, numbers, and symbols.
- Avoid common words; some hackers use programs that try every word in the dictionary.
- Never use personal information (your name, children's names, dates of birth, etc.) that someone might already know or easily obtain.
- If you believe your system has been compromised, change your passwords immediately.
- Use different passwords (or at least a variety of passwords) for each online account you access.
- If you must write down your passwords, keep them in a secure location away from your computer. Under no circumstances should you store them in a document on your computer!

Estimating Password-Cracking Times



Common words

Why do we want to avoid common words?

Some hackers use programs that try every word in the dictionary. Often times these tools use what's called a rainbow table.

Rainbow Tables

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack infeasible.

OR

Rainbow tables help hackers find your password quickly.

Where Do I begin?

Now that you know why the password needs to be strong, how do you make it practical?

You have taken years to create the habits needed for an 8 character passwords how do I make them stronger?

The Book Method

Pick a base word from a random page:

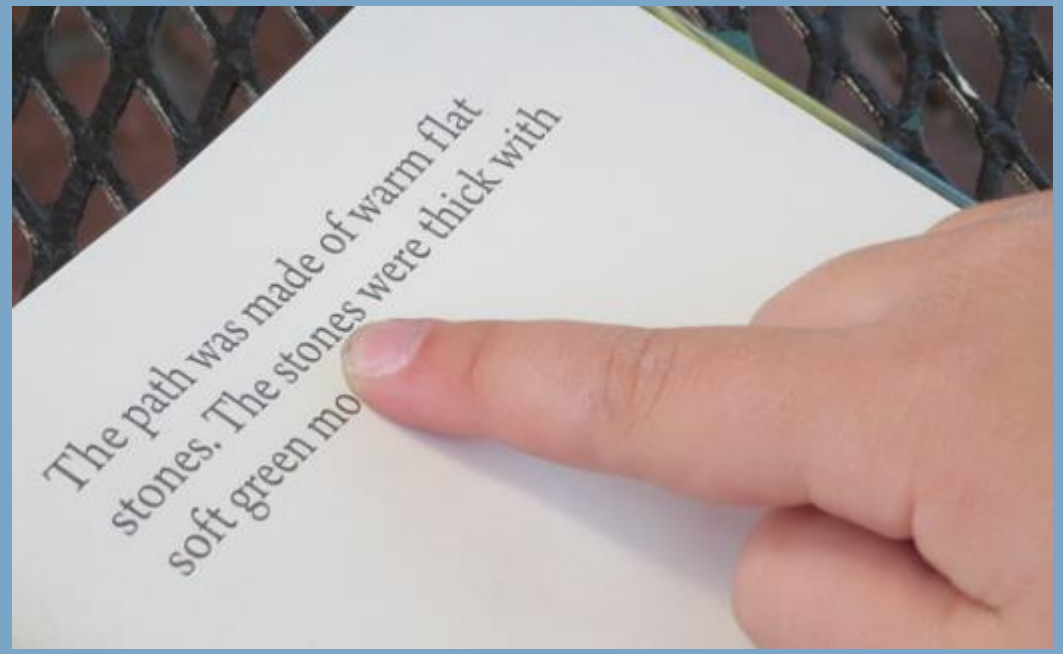
- Grab a small book you like.
- Flip to a random page and find a random word.
- Note the page number and where the word is located on the page.
- You can save the base word by underlining it and using a book mark.

The Book Method

Word: stones

Page: 106

Located: 2 line down 3 word in



Password:

106Stone23

First Letter Passphrase

Connect The First Letters Of A Passphrase:

This s a fun way to create passwords that are really easy to remember. Pick a phrase you love, such as “May the force be with you.”, and use the first letter of each word to create a new word: MTFBWY.

You can now use this base password in any number of creative ways. Some ideas are: reverse it, add numbers and/or symbols you’ll remember, or use first and last letters of each word (MyTeFeBeWhYu).

esreveR

Connect The First Letters Of A Passphrase:

Reversing words is an obvious yet effective way to create secure passwords. For example “Pickles and Ice cream”

By reversing this phrase to selkciPdnamaercecI or maercecIdnaselkciP, You get something that looks pretty much random, and is a much better fit for a base password.

Coded Passphrases

Changing letters some letters in a sentence to other characters.

a = @ e = 3 i = 1 o = 0 s = $

Some Examples:

1L0v3MyL1f3!

1@m@B1Gf@n

$h0wM3Th3$

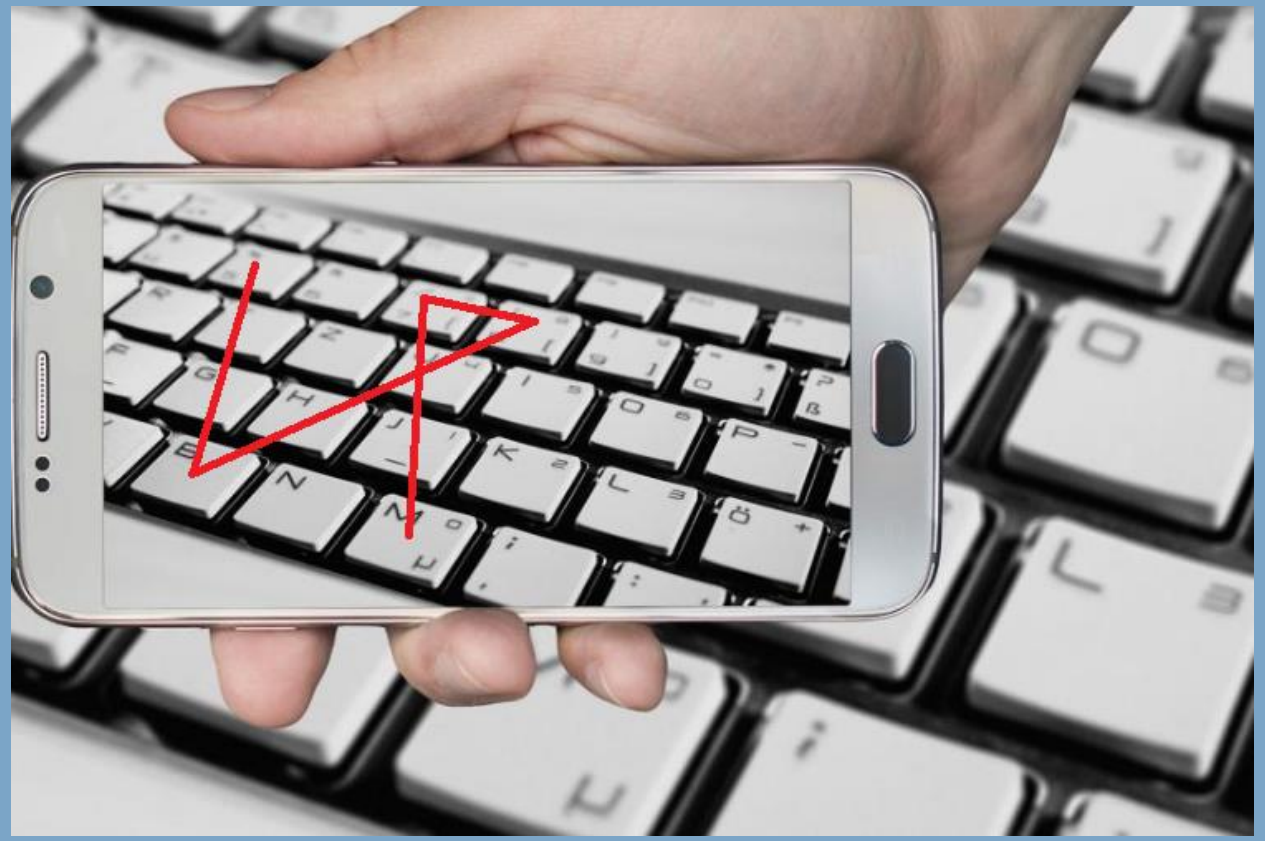
G@m30fThr0n3$

2B0rN0t2b?

MyJ0b1sGr8

$t@rW@r$f@n

Drawing with your keyboard



Touch Typist

Typing off F and J:

Some tips to make it easier

Making Different Passwords for Different sites:

Once you have your base password **********.

You need a way to have a different password for each site you go to.

Some tips to make it easier

Password Vaults

Work with Password Management Software

A password manager will:

- Generate passwords
- Retrieve passwords
- Keep track of super-long, crazy-random passwords across countless accounts
- PINs
- Answers to security questions
- Credit Card information
- Documentation

So how did we do?

- Passwords should have at *least* 10 characters, include uppercase and lowercase letters, numbers, and symbols.
- Avoid common words; some hackers use programs that try every word in the dictionary.
- Never use personal information (your name, children's names, dates of birth, etc.) that someone might already know or easily obtain.
- If you believe your system has been compromised, change your passwords immediately.
- Use different passwords (or at least a variety of passwords) for each online account you access.
- If you must write down your passwords, keep them in a secure location away from your computer. Under no circumstances should you store them in a document on your computer!

Want to learn more?

https://blog.hawksoft.com/tag/cybersecurity

"3 things agents should learn about cyber insurance and 4 steps to selling it."

"Deciphering Cybersecurity for Your Agency"

https://howsecureismypassword.net/